MODELO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA PROVINCIA DEL CHACO

2018

e-seguridad

CHACO
Gobierno del Pueblo

ANEXO

Modelo de Políticas de Seguridad de la Información de la Provincia del Chaco

Índice

1. Introducción

1.1 Alcance

La presente Política tiene como objeto gestionar la seguridad de la información, los sistemas informáticos y el ambiente tecnológico. Como así también a toda la planta de personal, sea cual fuere su nivel jerárquico y su situación de revista de las áreas de los organismos públicos.

1.2 Seguridad de la información

La información es un activo que, como otros activos importantes, es esencial y en consecuencia necesita ser protegido adecuadamente.

La información puede existir en muchas formas, impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación.

Por lo que siempre debiera estar apropiadamente protegida, cualquiera sea la forma que tome la misma, o medio por el cual sea almacenada o compartida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad de las operaciones, minimizar los riesgos y asegurar el funcionamiento normal del área.

La seguridad de la información se logra implementando un adecuado conjunto de medidas; incluyendo políticas, controles, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estas medidas cuando sea necesario para asegurar que se cumplan los objetivos de seguridad específicos. Estas medidas se deben realizar en conjunción con otros procesos de gestión del área.

1.3 Necesidad de Seguridad de la Información

Los resultados de la evaluación del riesgo (ver 1.5) ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos.

La evaluación del riesgo se debiera repetir periódicamente para tratar cualquier cambio que podría influir en los resultados del mismo.

La política de seguridad de la información debe proponer minimizar los riesgos en la gestión de la información preservando su confidencialidad, integridad y disponibilidad.

1.4 Requerimientos de seguridad

Se debe identificar los requerimientos de seguridad, los cuales provienen de tres fuentes principales:

- La primera se deriva de evaluar los riesgos para el área, alineándose con la estrategia general y a sus objetivos.
- La segunda, son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus suministradores de información, contratistas y proveedores de servicio; y su ambiente sociocultural.
- La tercera fuente proviene del conjunto particular de principios, objetivos y requerimientos funcionales para el procesamiento de la información que un área ha desarrollado para sostener sus operaciones.

1.5 Evaluación de los riesgos de seguridad

Los requerimientos de seguridad se identifican mediante una evaluación periódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño operacional probable resultado de fallas en la seguridad.

Se debe considerar que los controles en esta política son importantes y así determinar la relevancia de los riesgos a los que se enfrenta la organización diariamente. Por lo tanto, aunque el enfoque arriba mencionado es considerado como un buen punto de inicio, no reemplaza la selección de controles basada en la evaluación del riesgo.

1.6 Selección de controles

Una vez que se han identificado los requerimientos y los riesgos de seguridad y se hayan tomado las decisiones para el tratamiento de los riesgos, se debe seleccionar los controles apropiados que se deberían implementar para asegurar que los riesgos se reduzcan a un nivel aceptable.

La selección de los controles depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado a la organización, y también debieran estar sujetas a todas las regulaciones y legislación provinciales, nacionales e internacionales aplicables.

1.7 Punto de Inicio

Se pueden considerar un número de controles como un buen punto de inicio para la implementación de la seguridad de la información. Estos se basan en requerimientos legales esenciales o pueden ser considerados como una práctica común para la seguridad de la información.

Los controles considerados como esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación aplicable:

a) protección de datos y privacidad de la información personal,
b) protección de los registros organizacionales,
c) derechos de propiedad intelectual.

Los controles considerados práctica común para la seguridad de la información, incluyen:

a) documento de la política de seguridad de la información;
b) asignación de responsabilidades de la seguridad de la información;
c) conocimiento, educación y capacitación en seguridad de la información;
d) procesamiento correcto en las aplicaciones;
e) gestión de la vulnerabilidad técnica;
f) gestión de la continuidad operacional;
g) gestión de los incidentes y mejoras de la seguridad de la información.

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios.

La información y los procesos, sistemas y redes de apoyo son activos importantes. Definir, lograr, sostener y mejorar la seguridad de la información puede ser esencial para mantener una eficacia en la operación de las actividades del área, observancia legal e imagen.

Las organizaciones, sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o ataques de denegación servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para las actividades del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, las medidas de seguridad funcionaran como un facilitador; por ejemplo para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de un planeamiento cuidadoso y prestar atención a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de los diferentes grupos de interés, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

1.8 Factores críticos de éxito

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de un área:

a) política, objetivos y actividades de seguridad de información que reflejan los objetivos del área;
b) un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la información que sea consistente con la cultura organizacional;
c) soporte visible y compromiso de todos los niveles de gestión;
d) un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo;
e) comunicación efectiva de la seguridad de la información con todos los directores, empleados y otras partes para lograr conciencia sobre el tema;
f) distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los directores, empleados y otras partes involucradas;
g) provisión para el financiamiento de las actividades de gestión de la seguridad de la información, así como para la incorporación y mantenimiento de tecnologías, softwares y servicios;
h) proveer el conocimiento, capacitación, concientización y educación apropiados;
i) establecer un proceso de gestión de incidentes de seguridad de la información;
j) implementación de un sistema de medición que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento;
k) Recursos humanos abocados a esta tarea.

2. Términos y Definiciones

2.1 Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

1. **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
2. **Integridad**: se salvaguarda la exactitud y totalidad de la información, como así también, los métodos de procesamiento.
3. **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

1. **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
2. **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
3. **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
4. **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
5. **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el área.
6. **Confiabilidad de la Información**: se refiere a que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones.

1. **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
2. **Activo**: Algo que presenta valor para la organización.
3. **Activo de información**: Es todo aquello que comprende la información o los elementos que la contienen o permiten su procesamiento y en consecuencia, debe ser protegido.
4. **Activo primario**: Se remite a la información y procesos
5. **Activo de Soporte**: Son los que se incluyen dentro de hardware, software, redes, personal, sitio, servicio, etc.
6. **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
7. **Tecnología de la Información**: Se refiere al hardware y software operados por el área o por un tercero que procese información en su nombre, para llevar a cabo una función propia del área, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
8. **Propietario de la Información**: Debe ser entendido desde su acepción técnica, no jurídica, donde se define que es un individuo o entidad, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término “propietario” no significa que la persona disponga de los derechos de propiedad reales del activo.
9. **Terceros**: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

2.2 Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del área.

2.3 Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

2.4 Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

NOTA. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

2.5 Propietario del Riesgo

Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

2.6 Gabinete de Seguridad de la Información

El Gabinete de Seguridad de la Información estará integrado por las máximas autoridades de cada jurisdicción dependientes del Poder Ejecutivo y contará con la participación de un representante de la Dirección General de Tecnologías de la Información y Comunicación.

2.7 Comité Jurisdiccional de Seguridad de la Información

El Comité Jurisdiccional de Seguridad de la Información, es un cuerpo integrado por representantes de todos los procesos sustantivos del área, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.8 Puntos activos

Su creación estará supeditada a la consideración del Comité Jurisdiccional de Seguridad de la Información solamente en las jurisdicciones cuya magnitud u objetivo lo amerite.

2.9 Responsable de Seguridad de la Información

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del área que así lo requieran.

2.10 Incidente de Seguridad

Un incidente de seguridad es un evento adverso que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad, o un intento o amenaza de romper los mecanismos de seguridad existentes.

2.11 Riesgo

Combinación de la probabilidad de ocurrencia de un evento, o que una amenaza determinada explote las vulnerabilidades de los activos.

2.12 Amenaza (externo)

Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

2.13 Vulnerabilidad (interno)

Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

2.13 Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

NOTA. Control es también utilizado como sinónimo de salvaguarda o de contramedida.

2.14 Organismo

En el ámbito del presente modelo se define Organismo a las Jurisdicciones y oficinas que comprenden el Poder Ejecutivo Provincial, así como sus Organismos Autárquicos y a los Descentralizados.

2.15 Área

Lugar de aplicación de la presente política.

3. Estructura de la política Modelo

Este modelo que se divide en dos partes, y guarda la siguiente estructura:

1) Cuatro capítulos introductorios que incluyen:
   - Introducción
   - Términos y definiciones
   - Estructura de la Política Modelo
   - Evaluación y tratamiento de riesgos
2) Catorce cláusulas que abarcan los diferentes aspectos o dominios de la seguridad de la información. Se presentan de manera sistemática y consistente. Estas cláusulas o dominios son:
   1. Política de seguridad
   2. Organización
   3. Recursos humanos
   4. Gestión de activos
   5. Gestión de Accesos
   6. Criptografía
   7. Seguridad Física y Ambiental
   8. Seguridad de las operaciones
   9. Seguridad de las comunicaciones
   10. Adquisición, desarrollo y mantenimiento de sistemas
   11. Relaciones con Proveedores
   12. Gestión de Incidentes de seguridad de la información
   13. Gestión de continuidad
   14. Cumplimento

   Cada cláusula contiene un número de categorías o grupo de controles de seguridad principales. Por último, por cada categoría, se establece un objetivo y contiene uno o más controles a realizar. A modo de síntesis se enuncia a continuación la estructura de cada cláusula o dominio:
   - Generalidades
   - Objetivos
   - Alcance
   - Responsabilidades
   - Política
     - Categorías
     - Objetivo
     - Controles

4. Evaluación y tratamiento de riesgos

Generalidades

Si el área no conoce sobre el riesgo que corren sus activos de información, difícilmente llegará a estar preparada para evitar su posible ocurrencia, de allí la importancia de conocer el riesgo y crear controles para disminuirlo o eliminarlo.

Es por ello que resulta imprescindible gestionar los riesgos del área, como pilar fundamental para la gestión de seguridad.

Objetivo

Conocer el riesgo a los que están sometidos los activos es imprescindible para poder gestionarlos.

Alcance

Esta Política se aplica a toda la información administrada en el área, cualquiera sea el soporte en que se encuentre.

Responsabilidad

El Comité Jurisdiccional de Seguridad de la Información será responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo.

El Responsable de Seguridad de la Información junto con los Directivos del área, será responsable del desarrollo del proceso de gestión de riesgos de seguridad de la información.

Política

4.1 Evaluación de los riesgos de seguridad

El área evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación y de los objetivos de control relevantes para el mismo. Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo, por ejemplo: cambios producidos en activos, amenazas, vulnerabilidades, impactos, valoración de riesgos.

Asimismo, se debe efectuar la evaluación cada vez que ocurran cambios significativos. Es conveniente que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

El alcance de una evaluación de riesgos puede incluir a toda el área, una parte, un sistema de información particular, componentes específicos de un sistema, o servicios. Resulta recomendable seguir una metodología de evaluación de riesgos para llevar a cabo el proceso.

4.2 Tratamiento de riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, el área debe decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Los riesgos pueden ser aceptados si por ejemplo: se evaluó que el riesgo es bajo o que el costo del tratamiento no es económicamente viable para la organización. Tales decisiones deben ser tomadas por las autoridades y debidamente documentadas.

Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:

a) Mitigarlos mediante la aplicación de controles apropiados para reducirlos;
b) Aceptarlos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos del área;
c) Evitarlos, eliminando las acciones que dan origen a la ocurrencia de estos;
d) Transferirlos a asociados y a otras partes interesadas, por ejemplo: compañías de seguro o proveedores.
e) Establecer parámetros de clasificación y descripción de información estandarizados para reducir la pérdida, intercambio o flujo no deseado en la información. Así como se observan en los procesos archivísticos.

Para aquellos riesgos donde la decisión ha sido la mitigación, se buscará reducirlos a un nivel aceptable mediante la implementación de controles, teniendo en cuenta lo siguiente:

a) requerimientos y restricciones de legislaciones y regulaciones provinciales, nacionales e internacionales;
b) objetivos organizacionales;
c) requerimientos y restricciones operativas;
d) costo de implementación y operación en relación directa a los riesgos reducidos, y proporcionales a los requerimientos y restricciones del área;
e) la necesidad de equilibrar las inversiones en la implementación y operación de los controles contra el daño que podría resultar de las fallas de seguridad.

Los controles a implementar deben ser seleccionados del contenido de las cláusulas de esta política. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o a su ambiente, y podrían no ser aplicables en todas las áreas.

Se debe recordar que ningún conjunto de controles puede alcanzar la seguridad absoluta. Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad.

5. Cláusula: Política de Seguridad de la Información

Generalidades

La información debe ser vista como un recurso sustancial para las áreas públicas con igual valor al resto de los activos y por lo cual debe ser protegida.

Las políticas de Seguridad de la Información tienen como objetivo protegerla de una amplia gama de amenazas, con el fin de garantizar la continuidad de los sistemas de información y la operación de las mismas, minimizando los riesgos y asegurando el eficiente cumplimiento de los objetivos de éstas.

Por lo cual es de suma importancia que los principios de la Política de Seguridad sean parte vital de la cultura de la Organización. Para esto, se debe asegurar un compromiso manifiesto de las máximas autoridades del área para la difusión, consolidación y cumplimiento de la misma.

Objetivo

El objetivo de la presente política es proteger frente amenazas, internas o externas, premeditadas o accidentales, a los recursos de información y la tecnología utilizada para su tratamiento, con el objetivo de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y presupuestos correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Política de Seguridad del área actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Esta Política se aplica en todo el ámbito del área, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Responsabilidad

Es responsabilidad de todas las autoridades jerárquicas, autoridades políticas y personal técnico, la implementación de esta Política de Seguridad de la Información, como así también hacer cumplir dichas políticas a su equipo de trabajo o personal a cargo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del área, cualquiera sea su situación de revista, y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades del área aprueban la aplicación de esta Política y son responsables de la autorización de sus modificaciones.

Esquema Organizativo

1° Nivel: GABINETE DE SEGURIDAD DE LA INFORMACIÓN

Conformación:

- Estará integrada por las máximas autoridades o un representante designado, de cada jurisdicción dependiente del Poder Ejecutivo acompañado por el Responsable de Seguridad Jurisdiccional.
- Contará con un órgano técnico asesor representado por la Dirección General de Tecnologías de Información y Comunicación o cualquiera sea la denominación que adquiera en el futuro, que tendrá participación en las reuniones del Gabinete de Seguridad de la Información y cumplirá sus veces la función de Secretaria Ejecutiva.

Responsabilidades:

- Generar un ámbito de encuentro donde las partes puedan compartir experiencias y problemáticas a los efectos de definir estrategias conjuntas o específicas para el desarrollo de lineamientos que permitan atender los aspectos en materia de seguridad de la información.
- Promover en cada jurisdicción, a través de su máxima autoridad, la constitución de un Comité Jurisdiccional de Seguridad de la Información y llevar un registro de conformación.
- Ratificar el Modelo de Política de Seguridad de la Información.
- Habilitar un canal de comunicación on-line permanente con cada Comité Jurisdiccional de Seguridad de la Información que sirva como base de conocimientos y mantenga informado de los problemas de seguridad detectados y soluciones aplicadas.
- Reunirse al menos una vez al año a fin de evaluar la implementación de las políticas de seguridad de información y de tomar conocimiento de los incidentes de seguridad acontecidos.
- Velar por la formación del personal idóneo para que especialice en la materia.

2° Nivel: COMITÉ JURISDICCIONAL DE SEGURIDAD DE LA INFORMACIÓN

Conformación:

Todo ente u organismo debe, mediante el Comité Jurisdiccional de Seguridad de la Información, establecer, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de gestión de

seguridad de la Información. El Comité Jurisdiccional de Seguridad de la Información debe estar conformado por un equipo interdisciplinario de carácter transversal a la entidad donde por los agentes de la Jurisdicción/Organismo deberán ser designados por instrumento legal de la máxima autoridad jurisdiccional.

- Cada Comité Jurisdiccional de Seguridad de la Información contará como mínimo con los siguientes puestos:
    - Responsable de seguridad.
    - Responsable de recursos humanos.
    - Responsable de Legal.
    - Responsable de informática.

Responsabilidades:

- Elaborar, aprobar y revisar anualmente la Política de Seguridad de la Información.
- Monitorear cambios en los riesgos que afectan a los recursos de información frente a amenazas de mayor significancia.
- Intervenir, registrar. y monitorear los incidentes relativos a la seguridad.
- Acompañar e impulsar el desarrollo de proyectos de seguridad
- Promover iniciativas para incrementar la seguridad de la información en las distintas áreas de la jurisdicción, y procesos específicos relativos a seguridad de la información.
- Garantizar la implementación de mecanismos para que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y/o coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de la jurisdicción.
- Definir criterios y niveles de riesgo aceptables.

En caso que lo amerite, por magnitud o estrategia de implementación, este Comité Jurisdiccional podrá crear puntos activos en las áreas de la Administración Pública

Conformación:

- Cada punto activo contará como mínimo con los siguientes roles:
    - Coordinador del punto activo
    - Propietarios de la información

Responsabilidades:

- Tanto el punto activo como sus miembros tendrán las mismas responsabilidades que el Comité Jurisdiccional de Seguridad de la Información pero dentro de su ámbito orgánico.
- Propondrá al Comité Jurisdiccional de Seguridad de la Información, en caso de ser necesario, una adecuación a la Política de Seguridad de la Información, que incluya las particularidades de su ámbito orgánico.
- El coordinador del punto activo participará de las reuniones del Comité Jurisdiccional de Seguridad de la Información.

5.1 Categoría: Política de Seguridad de la información

Objetivo

Otorgar al Organismo la orientación y soporte sobre la seguridad de la información alineándose a las Leyes y Decretos vigentes, como así también a las Regulaciones establecidas por la Dirección General de

Tecnologías de Información y Comunicación. Con el fin de que el Organismo pueda establecer claramente las políticas en línea con sus objetivos.

5.1.1 Control: Conjunto de políticas para la seguridad de la información

El documento de la política debe ser aprobado por el Comité Jurisdiccional de Seguridad, publicado y comunicado a todos los empleados y las partes externas relevantes.

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la información, que incluyen los siguientes tópicos:

1. Organización de la Seguridad: Orientado a administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para controlar su implementación.
2. Recursos Humanos: Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Organismo o uso inadecuado de instalaciones.
3. Gestión de Activos: Destinado a mantener una adecuada protección de los activos del Organismo.
4. Control de Acceso: Orientado a controlar los accesos a la información por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.
5. Cifrado: Destinado al uso de sistemas y técnicas criptográficas para la protección de la información, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.
6. Física y Ambiental: Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información del Organismo.
7. Seguridad en la Operativa: Orientado a controlar la existencia de los procedimientos de operaciones, el desarrollo y mantenimiento de documentación actualizada relacionada.
8. Seguridad en las Telecomunicaciones: Dirigido a asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.
9. Adquisición. Desarrollo y Mantenimiento de los Sistemas: Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su adquisición, desarrollo y/o implementación y durante su mantenimiento.
10. Relación con los suministradores: Destinado a implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados con los acuerdos de entrega de servicios de terceros.
11. Gestión de Incidentes de seguridad: Orientado a administrar todos los eventos que atenten contra la confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos.
12. Gestión de Continuidad: Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.
13. Cumplimiento: Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

5.1.2 Control: Revisión de la política de seguridad de la información

La política de seguridad de la información debe tener un dueño, responsable de las actividades de desarrollo, evaluación y revisión de la política.

La actividad de revisión debe incluir las oportunidades de mejoras, en respuesta a los cambios, entre otros: organizacionales, normativos, legales, de terceros, tecnológicos.

Las mejoras tenidas en cuenta deben quedar registradas y tener las aprobaciones de los responsables.

El Comité Jurisdiccional de Seguridad de la Información debe realizar una revisión a intervalos planeados y prever el tratamiento de caso de los cambios no planeados, a efectos de mantener actualizada la política.

Asimismo efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

6. Cláusula: Organización

Generalidades

La siguiente Política de Seguridad instaura la administración de la seguridad de la información, como parte primordial de los objetivos y actividades del área.

Por lo que, se definirá formalmente el ámbito de gestión para realizar las tareas de aprobación, implementación y la asignación de funciones y responsabilidades de las Políticas.

Se debe tener en cuenta que algunas actividades del área requieren que terceros puedan acceder a información interna, o que ciertas funciones relacionadas con el procesamiento de la información sean realizadas por terceros. En dicho caso se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros no es adecuadamente administrado, por lo que se debe establecer las medidas adecuadas que permitan la protección de la información.

Objetivo

Administrar la seguridad de la información del área y establecer un marco que permita iniciar y controlar su implementación, la distribución de funciones y responsabilidades.

Fomentar la consulta y participación entre áreas para propiciar la colaboración y la cocreación en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del área.

Alcance

Esta Política se aplica a todos los recursos del área y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Política

6.1 Categoría: Organización interna

Objetivo

Manejar la seguridad de la información dentro del área.

Establecer el marco referencial, para iniciar y controlar la implementación de la seguridad de la información dentro del área.

6.1.1 Control: Asignación de responsabilidades de la seguridad de la información

Las funciones definidas para las responsabilidades asociadas a la seguridad de la información serán distribuidas de la siguiente manera:

El **Comité Jurisdiccional de Seguridad de la Información** tendrá a cargo la presentación para la aprobación de la presente Política, ante la máxima autoridad del organismo, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, promoción de procesos de concientización, etc.), la proposición de asignación de funciones y aprobará el protocolo de comunicación entre las áreas pertinentes.

El comité de seguridad realizará reuniones de manera periódica o cuando lo consideren necesario.

La participación de todos los integrantes es obligatoria, salvo que existan razones de fuerza mayor que lo impidan cada participante podrá designar un representante para la misma.

Cada reunión tratará los temas pendientes de reuniones anteriores, compromisos asumidos y otras cuestiones que se presenten en el temario del día.

De cada reunión surgirán recomendaciones que se especificarán en el documento correspondiente, el cual se elabora mensualmente.

En cada reunión se confeccionará una minuta sobre los temas tratados donde se plasmarán los compromisos asumidos. Los compromisos, tareas y asuntos asignados serán comunicados.

El **Responsable de Seguridad** que a su vez cumplirá las funciones de **Coordinador** será el responsable de impulsar la implementación de la presente Política, con el análisis de riesgo y plan de contingencia correspondiente, como así también su cumplimiento.

Convocar a los miembros del comité a las reuniones para la revisión de la política de seguridad y comunicación de incidentes de seguridad. Y a su vez actuará como secretario ejecutivo en las mismas.

Proponer a la máxima autoridad jurisdiccional dictamen sobre el tratamiento de los incidentes de seguridad.

Asistirá al personal del Organismo en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los propietarios de la información, elaborará propuestas de modificación y actualización de las políticas de seguridad de la información.

Promoverá su aprobación y llevará el seguimiento en el Comité Jurisdiccional de Seguridad de la Información. Apoyará y supervisará la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

Será responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el grado de cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

Monitorear el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.

Y será en encargado de notificar las incidencias en la base de conocimiento proporcionada por el Organismo competente (Dirección General de Tecnología de Información y Comunicación).

Los **Propietarios de la información** serán los responsables de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, actualizándola periódicamente. También definirá perfiles de usuarios y otorgará permisos de acceso a la información de acuerdo a sus funciones y competencia. Sin que ello implique la ostentación del dominio de la información.

El **Responsable del Área de Recursos Humanos** deberá notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Además comunicará al personal los cambios en la Política de seguridad de la información y realizará eventos de capacitación continua en materia de seguridad.

El **Responsable del Área Informática** deberá cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Jurisdicción. Llevará a cabo desarrollos y mantenimientos de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El **Responsable Legal** colaborará en la redacción de las Políticas de Seguridad de la información y notificará a quien corresponda sobre las modificaciones que se efectúen a la Política de Seguridad de la Información del Organismo.

Verificará el cumplimiento de la actual Política en la gestión de todos los contratos, acuerdos u otra documentación del Organismo con sus empleados y con terceros.

Asesorará al Comité frente a la existencia de violaciones a la presente Políticas.

6.1.2 Control: Segregación de Tareas

El Comité Jurisdiccional de seguridad de la información tendrá como responsabilidad aprobar el protocolo de comunicación entre las áreas sustantivas a la implementación de las Políticas de Seguridad de la Información.

Este protocolo deberá ser documentado y deberá encontrarse de manera accesible a todos los interesados.

6.1.3 Control: Contactos con las autoridades

El **Responsable de Seguridad** en su rol de **Coordinador del Comité Jurisdiccional** de la información será el encargado de establecer los contactos con las autoridades superiores y asesorar a las autoridades en las reuniones del Gabinete de Seguridad de la Información.

6.1.4 Control: Contacto con Grupo de Interés especial

El **Responsable de Seguridad** será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad el contacto con todas las Áreas o direcciones del Organismo.

Deberá ser referente y formar parte de grupos relacionados a la presente temática:

a) Adquirir nuevos conocimientos acerca de las mejores prácticas y estar actualizado;
b) Asegurar que la concientización acerca de la seguridad de la información esté actualizada y completa;

c) Recibir alertas tempranas, avisos y recomendaciones ante ataques y vulnerabilidades;
d) Proporcionar vínculos adecuados durante el tratamiento de los incidentes de seguridad de la información.

6.1.5 Control: Seguridad de Información en la gestión de proyectos

El Responsable de Seguridad de la información será el encargado de verificar la implementación de la seguridad de la información en la gestión de proyectos, independientemente del tipo de proyecto a desarrollar.

6.2 Categoría: Dispositivos para movilidad y teletrabajo

Objetivo

Garantizar la seguridad de la información en el uso de recursos móviles o de teletrabajo.

La protección debe estar en concordancia a los riesgos que el organismo decide aceptar con respecto a esta modalidad de trabajo.

Se deberá disponer de definiciones claras para la protección, no sólo de los propios equipos informáticos portátiles sino, en mayor medida, de la información almacenada en ellos.

6.2.1 Control: Políticas para el uso de dispositivos de movilidad

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura del Organismo.

Se debe tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible (celulares, tablets, notebooks, etc.), y a todos los dispositivos que pudieran contener información de carácter confidencial y por lo tanto, de ser pasibles de sufrir incidentes que comprometan la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

a) La protección física necesaria.
b) El acceso seguro a los dispositivos.
c) La utilización segura de los dispositivos en lugares públicos.
d) El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos.
e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
f) Los mecanismos de resguardo de la información contenida en los dispositivos.
g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia debe entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

a) Permanecer siempre cerca del dispositivo.
b) No dejar desatendidos los equipos.
c) No llamar la atención acerca de portar un equipo valioso.
d) No poner identificaciones del Organismo en el dispositivo, salvo los estrictamente necesarios.
e) No poner datos de contacto técnico en el dispositivo.
f) Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del Organismo, los que incluirán:

a) Revocación de las credenciales afectadas
b) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

Los dispositivos móviles de uso particular de los empleados no deberán ser utilizados para realizar trabajos en las oficinas salvo expresa autorización del Superior jerárquico, especificando los motivos.

6.2.2 Control: Teletrabajo

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al Organismo.

El trabajo remoto sólo será autorizado por el Superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad de la Información, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios del Organismo, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.
b) El ambiente de trabajo remoto propuesto.
c) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Organismo, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
d) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
e) Evitar la instalación / desinstalación de software no autorizado por el Organismo.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

7. Cláusula: Seguridad ligada a los recursos humanos

Generalidades

Es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad, ya que la seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

La implementación de la presente Política tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los contratos o cláusulas de confidencialidad a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y que estos se encuentren capacitados para respaldar la Política de Seguridad del área en el transcurso de sus tareas normales.

Establecer Contratos o cláusulas de Confidencialidad con todo el personal, contratistas y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Alcance

Esta Política se aplica a todo el personal del área, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito de la misma.

Responsabilidad

El Responsable del Área de Recursos Humanos informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Contratos de Confidencialidad con el personal acorde a las Disposiciones dictadas por la Dirección General de Recursos Humanos, y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

Política

7.1 Categoría: Antes de la contratación

Objetivo

Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las responsabilidades de seguridad deben ser tratadas antes del empleo en las definiciones de trabajo adecuadas y en los términos y condiciones del empleo.

7.1.1 Control: Investigación de antecedentes

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto, según la reglamentación vigente para la Administración Pública Provincial.

7.1.2 Control: Términos y condiciones de contratación

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del área. La copia firmada del Compromiso debe ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades, en su puesto de trabajo, que pueden ser objeto de control y monitoreo.

7.2 Categoría: Durante la contratación

Objetivo

Asegurar que los usuarios empleados cualquiera sea su situación de revista, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se deben definir las responsabilidades de las autoridades jerárquicas para asegurar que se apliquen los principios de seguridad a lo largo de todo el tiempo de duración del vínculo de la persona con el área, teniendo siempre en cuenta la normativa jurídica vigente.

7.2.1 Control: Responsabilidades de gestión

Es responsabilidad de la autoridad del área solicitar a los empleados cualquiera sea su situación de revista, contratistas y usuarios de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos por la organización, cumpliendo con lo siguiente:

a) estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se les otorgue el acceso a información sensible o a los sistemas de información;
b) ser provistos de guías para establecer las expectativas de seguridad de su rol dentro del área;
c) ser motivados para cumplir con las políticas de seguridad del área;
d) alcancen un nivel de conciencia sobre la seguridad acorde con sus roles y responsabilidades dentro del área;
e) cumplir con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del área y métodos adecuados de trabajo;
f) mantenerse con las habilidades y calificaciones adecuadas.

Si los empleados cualquiera sea su situación de revista, contratistas y usuarios no son conscientes de sus responsabilidades de seguridad, ellos pueden causar daños considerables al área. Un personal motivado tiene más probabilidades de ser más confiable y causar menos incidentes de seguridad de la información.

7.2.2 Control: Concienciación, educación y capacitación en seguridad de la información

Todos los empleados cualquiera sea su situación de revista del área y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la misma, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos que deben desarrollarse y aplicarse en el área. Esto comprende los requerimientos de seguridad y las

responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su puesto de trabajo.

El Responsable de Recursos Humanos o quien se encuentre a cargo de la capacitación interna del personal, será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

El personal que ingrese al área recibirá el material, indicándole el comportamiento esperado en lo que respecta a la seguridad de la información, antes de que le sean otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

7.2.3 Control: Proceso disciplinario

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales, aplicables de acuerdo a su situación de revista y, si correspondiera, se iniciaran las acciones penales conforme lo prescribe el Código Penal de la Nación Argentina, en su artículos 156, 157 y 157 bis, para los empleados que violen la Política, Normas y Procedimientos de Seguridad del área.

El proceso disciplinario también se puede utilizar como un elemento disuasivo para evitar que los empleados cualquiera sea su situación de revista, contratistas y terceros que violen las políticas y procedimientos de la seguridad del área y cualquier otro incumplimiento de la seguridad.

7.3 Categoría: Cese o cambio de puesto de trabajo

Objetivo

Asegurar que los usuarios empleados, contratistas y terceras personas, que por razones de cese del vínculo o transferencia del área en la cual prestan servicios, lo realicen en forma ordenada.

Se deben establecer las responsabilidades para asegurar que la desvinculación del área del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todos los equipos y se eliminen todos los derechos de acceso.

7.3.1 Control: Cese o cambio de puesto de trabajo

Las responsabilidades para realizar la desvinculación o cambio de puesto deben ser claramente definidas y asignadas y encontrarse acordes a lo indicado en la Ley N° 292-A (Antes Ley N° 2017), Ley N° 179-A (Antes Ley N° 1140), y Decreto N° 1311/99, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori y, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad, y los términos y condiciones de empleo con continuidad por un período definido de tiempo luego de la finalización del trabajo del empleado, contratista o usuario de tercera parte.

8. Cláusula: Gestión de activos

Generalidades

El área debe tener un conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

Se debe tener en cuenta que los activos a referir se tratan de los activos ligados a la información.

Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.
- Activos físicos: Libros, documentos de propiedad intelectual, artículos de arte, acervos histórico-culturales o cualquier otro elemento físico que contenga, administre o suministre información. Equipamiento informático, equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos —pendrives, discos externos, etc. —), otros equipos técnicos.
- Servicios: servicios informáticos y de comunicaciones, utilitarios generales.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Generalmente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en consecuencias innecesarios para el área.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

- Garantizar que los activos de información reciban un apropiado nivel de protección.
- Clasificar la información para señalar su sensibilidad y criticidad.
- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance

Esta Política se aplica a toda la información administrada en el área, cualquiera sea el soporte en que se encuentre.

Responsabilidad

Los propietarios de los activos son los encargados de clasificarlos de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, de definir las

funciones que deben tener permisos de acceso a los activos y son responsables de mantener los controles adecuados para garantizar su seguridad.

Todos los activos deben ser inventariados y contar con un responsable nombrado, acorde a lo que establece la Ley N° 1092-A (Antes Ley 4787) de Administración Financiera del Sector Público Provincial.

Responsable de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

Política

8.1 Categoría: Responsabilidad sobre los activos

Objetivo

Los propietarios deben identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos. Para los casos de los bienes muebles e inmuebles se deberá regir por lo establecido en la Ley N°1092-A (Antes Ley 4787) de Administración Financiera del Sector Público Provincial.

8.1.1 Control: Inventario de activos

Se identificarán los activos de información del área. Existen muchos tipos de activos, que incluyen:

a) información: bases de datos, archivos de datos, documentación, contratos, acuerdos;
b) activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios;
c) activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos;
d) instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua y gas, etc.;
e) servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, energía, y aire acondicionado;
f) personas, y sus calificaciones, habilidades y experiencia;
g) activos intangibles, tales como la reputación y la imagen del área.

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 12 meses.

El encargado debe elaborar el inventario y mantenerlo actualizado.

8.1.2 Control: Propiedad de los activos

Toda la información y los activos junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado en el área.

Se designarán los Propietarios de los activos identificados, quienes deben cumplir sus funciones de propietario, esto es:

a) informar sobre cualquier cambio que afecte el inventario de activos;
b) clasificar los activos en función a su valor;

c) definir los requisitos de seguridad de los activos;
d) velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de los activos será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

8.1.3 Control: Uso aceptable de los activos

Se identificarán, documentarán e implementarán reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información acorde a lo que establece la Ley N° 1092-A (Antes Ley 4787) de Administración Financiera del Sector Publico Provincial.

Todos los empleados, contratistas y usuarios de terceras partes deben seguir las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la misma, incluyendo:

a) correo electrónico,
b) sistemas de gestión,
c) estaciones de trabajo,
d) dispositivos móviles,
e) herramientas y equipamiento de publicación de contenidos,
f) otros.

8.1.4 Control: Devolución de activos

Todos los empleados y usuarios de terceras partes deberán devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.

8.2 Categoría: Clasificación de la información

Objetivo

Asegurar que la información reciba un nivel de protección apropiado.

La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Se debe utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

1) Control: Directrices de clasificación

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad. Se deberá tener en cuenta, también lo establecido en la Ley N° 1092-A (Antes Ley 4787) de Administración Financiera del Sector Público Provincial.

A continuación se establece la metodología de clasificación de la información propuesta en función a cada una de las mencionadas características:

Confidencialidad:

0. Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del área o no. PÚBLICO

1. Información que puede ser conocida y utilizada por todos los empleados del área y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el área, el Sector Público Provincial o terceros. RESERVADA - USO INTERNO

2. Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al área, al Sector Público Provincial o a terceros. RESERVADA - CONFIDENCIAL

3. Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del área, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Provincial o a terceros. RESERVADA SECRETA

Integridad:

0. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del área.

1. Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el área, el Sector Público Provincial o terceros.

2. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el área, el Sector Público Provincial o terceros.

3. Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al área, al Sector Público Provincial o a terceros.

Disponibilidad:

0. Información cuya inaccesibilidad no afecta la operatoria del área.

1. Información cuya inaccesibilidad permanente durante un plazo no menor a una semana, podría ocasionar pérdidas significativas para el área, el Sector Público Provincial o a terceros.

2. Información cuya inaccesibilidad permanente durante un plazo no menor a un día, podría ocasionar pérdidas significativas al área, al Sector Público Provincial o a terceros.

3. Información cuya inaccesibilidad permanente durante un plazo no menor a una hora podría ocasionar pérdidas significativas al área, al Sector Público Provincial o a terceros.

Al referirse a pérdidas, se contemplan aquellas mensurables (materiales) y no mensurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, otros).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

CRITICIDAD BAJA: ninguno de los valores asignados supera el 1.

CRITICIDAD MEDIA: alguno de los valores asignados es 2.

CRITICIDAD ALTA: alguno de los valores asignados es 3.

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, otros) y los perfiles funcionales que deben tener acceso a la misma.

En adelante se mencionara como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

2) Control: Etiquetado y manipulado de información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia;
- Almacenamiento;
- Transmisión por correo, fax, correo electrónico;
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, otros).
- Transmisión a través de mecanismos de intercambio de archivos (FTP, almacenamiento masivo remoto, otros).

Para cada uno de los niveles de clasificación, se deben definir los procedimientos de manejo seguros, incluyendo las actividades de procesamiento, almacenaje, transmisión, clasificación y destrucción.

3) Control: Manipulación de activos

Se deberán desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización y establecido en el ámbito de la Ley N° 1092-A (Antes Ley 4787) de Administración Financiera del Sector Publico Provincial.

8.3 Categoría: Manejo de los soportes de almacenamiento

Objetivo

Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades. Los medios se debieran controlar y proteger físicamente.

Se deben establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), entrada/salida de datos (input/output) y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción.

8.3.1 Control: Gestión de soportes extraíbles

El Responsable del Área Informática, con la asistencia del Responsable de Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, pendrives e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo a la cláusula "9.1 Categoría: Requerimientos para el Control de Acceso".

Se deben considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el área.
b) Requerir autorización para retirar cualquier medio del área y realizar un control de todos los retiros a fin de mantener un registro para la auditoría.

c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores y la criticidad de la información almacenada.

8.3.2 Control: Eliminación de soportes

El Responsable del Área Informática, junto con el Responsable de Seguridad de la Información definirá procedimientos para la eliminación segura de los medios de soporte de información respetando la normativa vigente.

Los procedimientos deben considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.
b) Voces u otras grabaciones.
c) Papel carbónico.
d) Informes de salida.
e) Cintas de impresora de un solo uso.
f) Cintas magnéticas.
g) Discos u otros dispositivos removibles.
h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
i) Listados de programas.
j) Datos de prueba.
k) Documentación del sistema.

La evaluación del mecanismo de eliminación debe contemplar el tipo de dispositivo y la criticidad de la información contenida.

8.3.3 Control: Soportes físicos en tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deben contemplar:

a) La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar, en conjunto con el Responsable de Seguridad, determinarán qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.
b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
    1. Uso de recipientes cerrados.
    2. Entrega en mano.
    3. Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).

En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

9. Cláusula: Control de Acceso

Generalidades

Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de

información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

En vista a que el acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática, por lo tanto es necesario concientizar a los usuarios acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Los procedimientos establecidos deben comprender todas las etapas del ciclo de vida de los accesos de los usuarios, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

Objetivo

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del área, cualquiera sea la función que desempeñe.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad

El Responsable de Seguridad de la Información estará a cargo de:

- Implementará las normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades (logs); y el ajuste de relojes de acuerdo a un estándar preestablecido, en conjunto con el Responsable del Área Informática. Esto deberá ser supervisado por el Comité de Seguridad.
- Proponer al Comité Jurisdiccional, pautas de utilización de Internet para todos los usuarios de acorde a los lineamientos establecidos por el Órgano Rector.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways y otros) y validarlos periódicamente.

- Controlar periódicamente la asignación de privilegios a usuarios asignados con anterioridad en conjunto con los Propietarios de la Información.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos (físicos y lógicos), subdivisión de redes, control de conexiones a la red, control de ruteo de red, y otros.
- En conjunto con el Responsable de Recursos Humanos, deberá concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar periódicamente el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
  - determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
  - definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
- Aprobar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

Los Propietarios de la Información junto al Responsable de la Seguridad de la información o en su defecto quien sea propuesto por el Comité Jurisdiccional de Seguridad de la Información o por los puntos activos, definirán un cronograma de depuración de logs y registros de auditoría en línea en función a normas vigentes y a sus propias necesidades.

El Responsable del Área Informática cumplirá las siguientes funciones en caso de ser necesario y acorde a los lineamientos del órgano rector:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Implementar el registro de eventos o actividades (logs) de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).

- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

El Comité Jurisdiccional de Seguridad de la Información o los coordinadores de los puntos activos, aprobarán el análisis de riesgos de la información efectuado. Asimismo, aprobarán el período definido para el mantenimiento de los registros de auditoría generados.

Política

9.1 Categoría: Requisitos de negocio para el control de accesos

Objetivo

Controlar el acceso a la información, medios de procesamiento de la misma y procesos sobre la base de los requerimientos del área y de seguridad. Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información y las leyes provinciales en la materia.

9.1.1 Control: Política de control de accesos

En la aplicación de gestión de acceso, se contemplarán los siguientes aspectos:

a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b) Identificar toda la información relacionada con las aplicaciones.
c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes (Ver cláusula 8 Gestión de Activos).
d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.

9.1.2 Control: Control de acceso a las redes y servicios asociados

Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

9.2 Categoría: Gestión de acceso de usuario

Objetivo

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de acceso a los sistemas, datos y servicios de información.

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información.

9.2.1 Control: Gestión de altas/bajas en el registro de usuario

El Responsable de Seguridad de la Información propondrá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del área, por ejemplo que no compromete la segregación de funciones.
d) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones y obligaciones para el acceso.
e) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
f) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
g) Cancelar inmediatamente los permisos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del área o sufrieron la pérdida/robo de sus credenciales de acceso.
h) Efectuar revisiones periódicas con el objeto de:
    - cancelar identificadores y cuentas de usuario redundantes
    - bloquear credenciales de usuarios inactivos por más de 90 días.
    - eliminar cuentas inactivas por más de un período no mayor a 120 días.
    - En el caso de existir excepciones, deben ser debidamente justificadas y aprobadas.
    - Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

9.2.2 Control: Gestión de los derechos de acceso asignados a usuarios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad de la Información.

9.2.3 Control: Gestión de los derechos de acceso con privilegios especiales

La asignación y uso de derechos de acceso con privilegios especiales deberá ser restringido y controlado.

Solo se habilitarán los mismos cuando cuente con la conformidad explícita y escrita de un Superior no inferior a Subsecretario o equivalente, el aval del Propietario de la Información y el Responsable de Seguridad de la Información.

9.2.4 Control: Gestión de información confidencial de autenticación de usuarios

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad.
b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez acreditada la identidad del usuario.
c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo formal cuando la reciban.
d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad de la Información conjuntamente con el Responsable del Área de Informática y el Propietario de la Información lo determinen necesario (o lo justifiquen).
f) Configurar los sistemas de tal manera que mínimamente cumplan los siguientes requisitos:
    - las contraseñas sean del tipo “password fuerte” y tengan una cantidad no menor a 8 caracteres
    - suspendan o bloqueen permanentemente al usuario luego de una cantidad no mayor a 3 a intentos de entrar con una contraseña incorrecta (debe pedir la rehabilitación ante quien corresponda),
    - solicitar el cambio de la contraseña en un lapso no mayor a 45 días,
    - impedir que las últimas 4 contraseñas sean reutilizadas.

9.2.5 Control: Salida fuera de las dependencias del Organismo

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares de 6 meses, a fin de revisar los derechos de acceso de los usuarios. Se deben contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios.

b) Revisar las autorizaciones de privilegios especiales de derechos de acceso.
c) Revisar las asignaciones de privilegios.

9.2.6 Control: Retirada o adaptación de los derechos de acceso

El Responsable de Seguridad de la Información en conjunto con el Órgano Rector, será el encargado de retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

9.3 Categoría: Responsabilidades del usuario

Objetivo

Evitar el acceso de usuarios no autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

9.3.1 Control: Uso de información confidencial para la autenticación

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable de Seguridad de que se trate, que:
    1. Sean fáciles de recordar.
    2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
    3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”).
f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
g) Notificar de acuerdo a lo establecido en la cláusula 16 Gestión de Incidentes de Seguridad, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

9.4 Categoría: Control de acceso a sistemas y aplicaciones

Objetivo

Evitar el acceso no autorizado a los servicios de la red.
Se debe controlar el acceso a los servicios de redes internas y externas.
El acceso del usuario a las redes y sus servicios no deben comprometer la seguridad de los servicios de la red asegurando:

a) que existan las interfaces apropiadas entre la red del área y las redes de otras organizaciones, y redes públicas;
b) se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;
c) el control del acceso del usuario a la información sea obligatorio.

9.4.1 Control: Restricción del acceso a la información

Se deberá restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

9.4.2 Control: Procedimientos seguros de inicio de sesión

Cuando sea requerido por la política de control de accesos se deberá controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on.

9.4.3 Control: Gestión de contraseñas de usuario

Los sistemas de gestión de contraseñas deberán ser interactivos y asegurar contraseñas de calidad.

9.4.4 Control: Uso de herramientas de administración de sistemas

El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas estará restringido y estrechamente controlado.

9.4.5 Control: Control de acceso al código fuente de los programas

Se deberá restringir el acceso de los usuarios al código fuente de las aplicaciones software.

10. Cláusula: Cifrado

Generalidades

La criptografía es una ciencia que hace uso de métodos y herramientas matemáticas con el objetivo principal de cifrar y por lo tanto proteger, un archivo por medio de un algoritmo, con el fin de lograr la confidencialidad y la autenticidad del mismo.

Esta técnica se usa en forma primaria para proteger la información de los riesgos de seguridad evitando que pueda ser interceptada por cualquier persona no autorizada.

Objetivo

Hacer uso de sistemas y técnicas criptográficas para proteger la información, con el fin de asegurar la adecuada protección de su confidencialidad e integridad.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el área en donde residan los desarrollos mencionados.

Responsabilidad

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad de la información definirá junto con el Responsable del Área de Sistemas o de quien sea competencia, los métodos de encripción a ser utilizados.

Asimismo, el Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

Política

10.1 Categoría: Controles criptográficos

Objetivo

Se utilizarán controles criptográficos con el objetivo de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas.

Las áreas deberán utilizar los controles criptográficos para proporcionar protección a las claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.

El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado.

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos y, en algunas ocasiones, podría ser necesario asesoramiento legal para establecer acuerdos especiales que respalden su uso.

10.1.1 Control: Política de uso de controles criptográficos

El área establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

1. Se utilizarán controles criptográficos en los siguientes casos:
   a) Para la protección de claves de acceso a sistemas, datos y servicios.
   b) Para la transmisión de información clasificada, fuera del ámbito del área.
   c) Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad de la Información.
2. Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

3. Se recomienda verificar periódicamente los algoritmos y longitudes seguros con el objeto de efectuar las actualizaciones correspondientes.

10.1.2 Control: Gestión de claves

Toda la información y los activos junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado en el área.

Se deberá desarrollar e implementará un sistema de administración de claves criptográficas a través de todo su ciclo de vida.

Donde se deberán redactarán las normas y procedimientos necesarios para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
b) Generar y obtener certificados de clave pública de manera segura.
c) Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.
d) Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
f) Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula del área (en cuyo caso las claves también deben archivarse).
g) Recuperar claves perdidas o alteradas como parte de la administración de la continuidad de las actividades del área, por ejemplo para la recuperación de la información cifrada.
h) Archivar claves, por ejemplo, para la información archivada o resguardada.
i) Destruir claves.
j) Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que los usuarios que no utilicen sus claves dentro de 3 meses quedarán bloqueados de forma automática y deberán solicitar el correspondiente desbloqueo. Asimismo, cada 12 meses el/los sistemas deberá/n solicitar la modificación de las claves.

Además de la administración segura de las claves secretas y privadas, debe tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa al propietario del par de claves pública/privada con la clave pública.

En consecuencia es importante que el proceso de administración de los certificados de clave pública sea absolutamente confiable. Este proceso deberá ser llevado a cabo por una entidad denominada Autoridad de Certificación (AC) o Certificador.

11. Cláusula: Seguridad física y ambiental

Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del área. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta:

a) La protección física de accesos

b) La protección ambiental y el transporte
c) La protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del área, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del área como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del Organismo. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al área pero situado físicamente fuera del mismo (“housing”) así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al área Organismo (“hosting”).

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación; y para su destrucción cuando así lo amerite.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del área.

Proteger el equipamiento destinado al procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del área.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.
Proporcionar protección proporcional a los riesgos identificados.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información del área: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, otros.

Responsabilidad

El Responsable de Seguridad de la Información definirá las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación.

Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en la presente Cláusula.

El Responsable del Área Informática y los Propietarios de la Información asistirán al Responsable de Seguridad de la Información en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de dichas áreas.

El Responsable de Seguridad de la Información será el encargado de revisar los registros de acceso a las áreas protegidas.

Política

11.1 Categoría: Áreas seguras

Objetivo

Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, de daños e interferencias.

11.1.1 Control: Perímetro de seguridad física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes del área y de las instalaciones de procesamiento de información.

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidos por los Propietarios de la Información con el asesoramiento del Responsable de Seguridad de la Información y el Responsable del Área Informática, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

a) Definir y documentar claramente el perímetro de seguridad.
b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
c) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán medios alternativos de control de acceso físico al área o edificio. El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.

d) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
e) Identificar claramente todas las salidas de emergencia de un perímetro de seguridad.

Un área segura puede ser una oficina con llave, o varias oficinas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad, dentro del mismo perímetro de seguridad

El Responsable de Seguridad de la Información llevará un registro actualizado de los sitios protegidos, indicando:

a) Identificación del Edificio y Área.
b) Principales elementos a proteger.
c) Medidas de protección física

11.1.2 Control: Controles físicos de entrada

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad de la Información junto con el Responsable del Área Informática y los Propietarios de la Información, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se mantendrá un registro protegido para permitir auditar todos los accesos.
c) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
d) Revisar y actualizar cada un período no mayor a 6 meses o cuando se requiera los derechos de acceso a las áreas protegidas, los que serán documentados y firmados.
e) Revisar los registros de acceso a las áreas protegidas.

11.1.3 Control: Seguridad de oficinas, despachos, instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad emitidas por los Entes competentes en la materia. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
e) Implementar mecanismos de control para la detección de intrusos. Los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.
f) Separar las instalaciones de procesamiento de información administradas por el Organismo de aquellas administradas por terceros.
g) Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas del Organismo. Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.
h) Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

11.1.4 Control: Protección contra amenazas externas y ambientales

Se debe prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

Se debe considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

a) los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no deben almacenarse en el área asegurada;
b) el equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal.
c) se debe proporcionar equipo contra-incendios ubicado adecuadamente.

11.1.5 Control: Trabajo en áreas seguras

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.
c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.
e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicha área o el Responsable del Área Informática y el Responsable de Seguridad de la Información.
g) Prohibir comer, beber y fumar dentro de las instalaciones.

11.1.6 Control: Áreas de acceso público, de carga y descarga

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados
Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Organismo, sólo al personal previamente identificado y autorizado.
b) Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
c) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.
d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
e) Registrar el material entrante al ingresar al sitio pertinente.
f) Cuando fuese posible, el material entrante debe estar segregado o separado en sus diferentes partes que lo constituyan.

11.2 Categoría: Seguridad de los equipos

Objetivo

Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades del Organismo.

Se debe proteger el equipo de amenazas físicas y ambientales.

11.2.1 Control: Emplazamiento y protección de equipos

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:
    - Amenazas potenciales
    - Robo o hurto
    - Incendio
    - Explosivos
    - Humo
    - Inundaciones o filtraciones de agua (o falta de suministro)

- Polvo
- Vibraciones
- Efectos químicos
- Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)
- Radiación electromagnética
- Derrumbes
- Etc.

e) Se deben establecer lineamientos sobre las actividades de comer, beber y fumar en la proximidad de los medios de procesamiento de la información.

f) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información.

g) Se deben aplicar protección contra rayos a todos los edificios y se deben adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.

11.2.2 Control: Instalaciones de suministro

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
b) Contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del Organismo. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Debe realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra

descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

Las opciones para lograr la continuidad de los suministros de energía incluyen múltiples alimentaciones para evitar que una falla en el suministro de energía.

11.2.3 Control: Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, asegurándose el cumplimiento de las normas y estándares dictados por la Dirección General de Tecnologías de la Información.

11.2.4 Control: Mantenimiento de los equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área Informática. El Área de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
d) Registrar el retiro de equipamiento de la sede del Organismo para su mantenimiento.
e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

11.2.5 Control: Salida fuera de las dependencias del Organismo

Los equipos, la información o el software no se deberán retirar del sitio sin previa autorización.

11.2.6 Control: Seguridad de los equipos y activos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del Organismo, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, debe ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del Organismo para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Organismo, cuando sea conveniente.

Los riesgos de seguridad, por ejemplo: daño, robo o intercepción; puede variar considerablemente entre los edificios y se debe tomarlo en cuenta para evaluar los controles apropiados.

11.2.7 Control: Reutilización o retirada segura de dispositivos de almacenamiento

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

Los dispositivos que contengan información confidencial deben requerir una evaluación de riesgo para determinar si los ítems debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

11.2.8 Control: Equipo informático de usuario desatendido

Los usuarios se deberán asegurar de que los equipos no supervisados cuentan con la protección adecuada.

11.2.9 Control: Política de puesto de trabajo despejado y bloqueo de pantalla

Se deberá adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.

12. Cláusula: Seguridad en la operativa

Generalidades

Se deben adoptar medidas de prevención, a favor de proteger la información evitado la ocurrencia de amenazas. Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Alcance

Todas las instalaciones de procesamiento de información del Organismo.

Responsabilidad

El Responsable de Seguridad de la información tendrá a su cargo, entre otros:

- Definir en conjunto con líder de proyecto y/o jefe de área los procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.

- Proponer criterios de aprobación para el desarrollo o implementación de nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para todas las aplicaciones.

- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.

- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo.

- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Responsable del Área Informática tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de operaciones.

- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.

- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.

- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.

- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración

- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.

- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).

- Administrar de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos

- Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

El Responsable de Seguridad de la información junto con el Responsable del Área Informática y el Responsable Legal del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información y el Responsable del Área Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

El Responsable de Seguridad de la información revisará las actividades que no hayan sido posibles segregar. Asimismo, revisará los registros de actividades del personal operativo.

Política

12.1 Categoría: Responsabilidades y procedimientos de operación

Objetivo

Asegurar la operación correcta y segura de los medios de procesamiento de la información.

Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados.

12.1.1 Control: Documentación de los procedimientos de operación

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad de la Información.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a) Procesamiento y manejo de la información.

b) Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.

c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.

d) Restricciones en el uso de utilitarios del sistema.

e) Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.

f) Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.

g) Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

a) Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.

b) Instalación y mantenimiento de las plataformas de procesamiento.

c) Monitoreo del procesamiento y las comunicaciones.

d) Inicio y finalización de la ejecución de los sistemas.

e) Programación y ejecución de procesos.

f) Gestión de servicios.

g) Resguardo de información.

h) Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.

i) Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.

j) Uso del correo electrónico.

12.1.2 Control: Gestión de cambios

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio debe ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se tendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

a) Identificación y registro de cambios significativos.

b) Evaluación del posible impacto de cambios.

c) Aprobación formal de los cambios propuestos.

d) Planificación del proceso de cambio.

e) Prueba del nuevo escenario.

f) Comunicación de detalles de cambios a todas las personas pertinentes.

g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

12.1.3 Control: Gestión de capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información del Organismo para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

12.1.4 Control: Separación de entornos de desarrollo, pruebas y operacionales

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado productivo.

Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de producción, en diferentes ambientes de operaciones, equipos, o directorios.

b) Separar las actividades de desarrollo y prueba, en entornos diferentes.

c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.

d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.

e) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.

f) El personal de desarrollo no tendrá acceso al ambiente productivo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

12.2 Categoría: Protección contra código malicioso

Objetivo

Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, bombas lógicas, etc. Los usuarios deben estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, los gerentes deben introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

12.2.1 Control: Control contra el código malicioso

El Responsable de Seguridad de la Información definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área Informática, o el personal designado por éste, implementará dichos controles.

El Responsable de Seguridad de la Información desarrollará procedimientos adecuados contemplen las siguientes acciones:

a) Prohibir la instalación y uso de software no autorizado por el Organismo (Ver 18.1.2 Control: Derecho de Propiedad Intelectual).

b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio (ej: dispositivos portátiles), señalando las medidas de protección a tomar.

c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.

d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).

e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del Organismo, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.

f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

h) Redactar normas de protección y habilitación de puertos de conexión de dispositivos móviles y sus derechos de acceso.

12.3 Categoría: Copias de seguridad

Objetivo
Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Se deben establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia (ver Cláusula 17.1 Categoría: Gestión de Continuidad del Organismo) para tomar copias de respaldo de los datos y practicar su restauración oportuna.

12.3.1 Control: Copias de seguridad de la información

El Responsable del Área Informática, de Seguridad de la Información y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Responsable del Área Informática dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración e integridad. Para esto se debe contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Organismo. Los sistemas de resguardo deben probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del organismo (ver Cláusula 17.1 Categoría: Gestión de Continuidad del Organismo).

Se definirán procedimientos para el resguardo de la información, que deben considerar los siguientes puntos:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.

c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas, y los procedimientos documentados de restauración a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deben tener al menos tres generaciones o ciclos de información de resguardo esenciales para el Organismo. Para la definición de información mínima a ser resguardada en el sitio remoto se debe tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad y requisitos legales a los que se encuentre sujeta.

d) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.

e) Probar periódicamente los medios de resguardo.

f) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

12.4 Categoría: Registro de actividad y supervisión

Objetivo
Detectar las actividades de procesamiento de información no autorizadas.

Se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información. Se deben utilizar bitácoras de operador y se deben registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información. Una organización debe cumplir con todos los requerimientos legales relevantes aplicables a sus actividades de monitoreo y registro.

Se debe utilizar el monitoreo del sistema para chequear la efectividad de los controles adoptados y para verificar la conformidad con un modelo de política de acceso.

12.4.1 Control: Registro y gestión de eventos de actividad

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para permitir la detección e investigación de incidentes.

Se debe evaluar la registración, en los mencionados registros, de la siguiente información:

a) identificación de los usuarios;

b) fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión;

c) identidad del equipo o la ubicación si es posible;

d) registros de intentos de acceso al sistema, exitosos y fallidos;

e) registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;

f) cambios a la configuración del sistema;

g) uso de privilegios;

h) uso de utilitarios y aplicaciones de sistemas;

i) archivos accedidos y el tipo de acceso;

j) direcciones de redes y protocolos;

k) alarmas que son ejecutadas por el sistema de control de accesos;

l) activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.

12.4.2 Control: Protección de los registros de información

Se implementarán controles para la protección de los registros de auditoría contra cambios no autorizados y problemas operacionales, incluyendo:

a) alteraciones de los tipos de mensajes que son grabados;

b) edición o eliminación de archivos de registro

c) exceso de la capacidad de almacenamiento de los archivos de registro, resultando en la falla para registrar los eventos o sobrescribiendo eventos registrados en el pasado.

12.4.3 Control: Registro de actividad del administrador y operador del sistema

Se registrarán y revisarán periódicamente en particular las actividades de los administradores y operadores de sistema incluyendo:

a) cuenta de administración u operación involucrada;

b) momento en el cual ocurre un evento (éxito o falla);

c) información acerca del evento (por ejemplo, los archivos manipulados) o las fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);

d) procesos involucrados.

12.4.4 Control: Sincronización de relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deben tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

12.5 Categoría: Control de Software en explotación

Objetivo

Garantizar la seguridad de los archivos del sistema.

Se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI. Asimismo, las actividades de soporte se debieran realizar de una manera segura.

12.5.1 Control: Instalación de software en sistemas de producción

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único Responsable propuesto por el Responsable del Área Informática.

- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de “implementador” al personal de su área que considere adecuado, quien tendrá como funciones principales:

- Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

- Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.

- Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.

- Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

a) Guardar sólo los ejecutables en el ambiente de producción.

b) Llevar un registro de auditoría de las actualizaciones realizadas.

c) Retener las versiones previas del sistema, como medida de contingencia.

d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformidades pertinentes, las pruebas previas a realizarse, etc.

e) Denegar, cuando correspondiere, permisos de modificación al implementador sobre los programas fuentes bajo su custodia.

Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

12.6 Categoría: Gestión de la vulnerabilidad técnica

Objetivo

Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

12.6.1 Control: Gestión de vulnerabilidades técnicas

Se obtendrá información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, la exposición del Organismo a tales vulnerabilidades evaluadas, y se tomarán las medidas necesarias para tratar los riesgos asociados.

Para ello se contará con un inventario de software donde se detalle información de versiones del mismo así como datos del proveedor y responsable interno.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;

b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;

c) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;

d) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;

e) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;

f) Identificación de los riesgos asociados a la instalación de parches;

g) Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;

h) Consideración de controles alternativos en caso de inexistencia de parches;

i) Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;

j) Seguimiento y evaluación regular del procesode gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia;

12.6.2 Control: Restricciones en la instalación de software

Se deben establecer e implementar:

- las reglas que rigen la instalación de software por parte de los usuarios y poner en vigencia una política estricta sobre qué tipo de software pueden instalar los usuarios.

La instalación no controlada de software en dispositivos computacionales puede dar pie a la introducción de vulnerabilidades y a la fuga de información, a la falta de integridad u otros incidentes de seguridad de información o bien a la transgresión de derechos de propiedad intelectual.

12.7 Categoría: Consideraciones de las auditorías de los sistemas de información

Objetivo

Asegurar el cumplimiento de minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

12.7.1 Control: Controles de auditoría de los sistemas de información

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

a) Acordar con el Área que corresponda los requerimientos de auditoría.

b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.

c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:

- Eliminar archivos transitorios.
- Eliminar entidades ficticias y datos incorporados en archivos maestros.
- Revertir transacciones.
- Revocar privilegios otorgados.

d) Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto quien sea propuesto por el Comité de Seguridad de la Información completará el siguiente formulario modelo, el cual debe ser puesto en conocimiento de las áreas involucradas:

Recursos de TI a utilizar en la verificación

Oficina

…….

Sistemas de información

…….

Base de datos

…….

Hardware

…….

Software de Auditoría

…….

Medios magnéticos

…….

Personal de Auditoría

…….

Interlocutores de las Áreas de Informática

…….

Interlocutores de las Áreas Usuarias

…….

Conexiones de Red

…….

e) Identificar y acordar los requerimientos de procesamiento especial o adicional.

f) Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:

- Fecha y hora.
- Puesto de trabajo.
- Usuario.
- Tipo de acceso.
- Identificación de los datos accedidos.
- Estado previo y posterior.
- Programa y/o función utilizada.

g) Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades

13. Cláusula: Seguridad en las telecomunicaciones

Generalidades

Los sistemas de información están comunicados entre sí, tanto dentro del Organismo como con terceros fuera de él. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Alcance

Todas las instalaciones de procesamiento y transmisión de información del Organismo.

Responsabilidad

El Responsable de Seguridad de la información tendrá a su cargo, entre otros:

- Controlar los mecanismos de distribución y difusión de información dentro del Organismo.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.
- El Responsable del Área Informática en conjunto con el Responsable de Seguridad tendrá a su cargo lo siguiente:
    - Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones.
    - Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
    - Implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.
- El Responsable de Seguridad de la información junto con el Responsable del Área Informática y el Responsable Legal del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.
- Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información y el Responsable del Área Informática, determinará los requerimientos para resguardar la información por la cual es responsable.

Política

13.1 Categoría: Gestión de la seguridad en las Redes

Objetivo

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicancias legales, monitoreo y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

13.1.1 Control: Controles de Red

El Responsable de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias.

b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable del Área Informática implementará dichos controles.

13.1.2 Control: Mecanismos de seguridad asociados a servicios en red

Se deberán identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.

13.1.3 Control: Segregación de redes

Se deberán segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.

13.2 Categoría: Intercambio de información con partes externas

Objetivo

Mantener la seguridad en el intercambio de información dentro del Organismo y con cualquier otra entidad externa.

Los intercambios de información dentro de las organizaciones se deben basar en una política formal de intercambio, seguida en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante (ver 18 Cláusula: Cumplimiento).

Se deben establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en tránsito.

13.2.1 Control: Políticas y procedimientos de intercambio de información

Se establecerán procedimientos y controles formales para proteger el intercambio de información a través del uso de todos los tipos de instalaciones de comunicación, considerando lo siguiente:

a) Protección de la información intercambiada por intercepción, copiado, modificación, de que sea mal dirigida, y de su destrucción.

b) Detección y protección contra el código malicioso.

c) Definición del uso aceptable de las instalaciones de comunicación electrónicas.

d) Uso seguro de comunicaciones inalámbricas.

e) Responsabilidades del empleado, contratista y cualquier otro usuario de no comprometer a la organización.

f) Uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información.

g) Directrices de retención y eliminación para toda la correspondencia en concordancia con las leyes y regulaciones relevantes, locales y nacionales.

h) Instrucción del personal sobre las precauciones que deben tomar a la hora de transmitir información del Organismo.

13.2.2 Control: Acuerdos de intercambio

Cuando se realicen acuerdos entre Organismos para el intercambio de información y software, se especificarán el grado de sensibilidad de la información del Organismo involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.

b) Procedimientos de notificación de emisión, transmisión, envío y recepción.

c) Normas técnicas para el empaquetado y la transmisión.

d) Pautas para la identificación del prestador del servicio de correo.

e) Responsabilidades y obligaciones en caso de pérdida, exposición o divulgación no autorizada de datos.

f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.

g) Términos y condiciones de la licencia bajo la cual se suministra el software.

h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.

i) Normas técnicas para la grabación y lectura de la información y del software.

j) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

13.2.3 Control: Mensajería electrónica

La mensajería electrónica como el correo electrónico, el intercambio de datos electrónicos (EDI por sus siglas en inglés), la mensajería instantánea y las redes sociales juegan un rol muy importante en las comunicaciones organizacionales. La mensajería electrónica tiene diferentes riesgos que las comunicaciones basadas en papel.

Se considerarán las siguientes medidas de seguridad en los mensajes electrónicos:

- protección de mensajes por el acceso no autorizado, modificaciones o denegación de servicio;
- correcta asignación de la dirección y el transporte del mensaje;
- confiabilidad y disponibilidad general del servicio;
- consideraciones legales, por ejemplo, requerimientos para firmas electrónicas;
- obtención de aprobación previa al uso de los servicios públicos externos tales como mensajería instantánea o el compartir archivos;
- niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.
- backups necesarios para recuperar información en caso de pérdida de información de buzón de usuario

13.2.4 Control: Acuerdos de confidencialidad y secreto

Se definirán, implementarán y revisarán regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información del Organismo. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación del Organismo, los cuales serán revisados periódicamente. Asimismo, deben cumplir con toda legislación o normativa que alcance al Organismo en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal del organismo como con aquellos terceros que se relacionen de alguna manera con su información.

14. Cláusula: Adquisición, desarrollo y mantenimiento de los sistemas de información

Generalidades

Durante el análisis y diseño de los procesos que soportan estos sistemas se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deben diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los sistemas se asientan sobre este tipo de software.

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Alcance
Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el área en donde residan los desarrollos mencionados.

Responsabilidad
El Responsable de Seguridad de la Información junto con el Propietario de la Información, propondrán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

Asimismo, el Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Establecer los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Proponer procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Responsable del Área Informática, propondrá al Comité Jurisdiccional de Seguridad de la Información, la asignación de funciones de “implementador” y “administrador de programas fuentes” al personal de su área que considere adecuado, cuyas responsabilidades deberán ser detalladas y encontrarse documentadas. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

Política

14.1 Categoría: Requisitos de seguridad de los sistemas de información

Objetivo
Garantizar la seguridad integral en los sistemas de información.

El diseño e implementación del sistema de información es crucial para la seguridad y se deben identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

14.1.1 Control: Análisis y especificación de los requisitos de seguridad
Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requisitos para nuevos sistemas o mejoras a los existentes determinarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

a) Cumplir los procedimientos definidos por el Órgano Rector en la materia durante las etapas de análisis y diseño del sistema.
b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.

c) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

14.1.2 Control: Seguridad de las comunicaciones en servicios accesibles por redes públicas

Se deben establecer los mecanismos necesarios para respaldar la integridad de la información disponible en los servicios de aplicación que pasan a través de redes públicas, con el fin de proteger contra actividades fraudulentas y/o de modificación no autorizada.

14.1.3 Control: Protección de las transacciones por redes telemáticas

Las transacciones de información de los servicios de las aplicaciones se deberá ser proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción que altere la integridad de los datos publicados.

Todos los sistemas de acceso público deben prever que:

a) La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley de Protección de Datos Personales.
b) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.
c) La información sensible o confidencial sea protegida durante el proceso de recolección y su almacenamiento.
d) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta este.
e) El responsable de la publicación de información en sistemas de acceso público sea claramente identificado.
f) La información se publique teniendo en cuenta las normas establecidas al respecto.
g) Se garantice la validez y vigencia de la información publicada.

14.2 Categoría: Seguridad en los procesos de desarrollo y soporte

Objetivo

Garantizar la incorporación de medidas seguridad durante todo el desarrollo de los sistemas, desde la fase de concepción hasta la desaparición del mismo.

14.2.1 Control: Política de desarrollo seguro de software

Se deberán aplicar los procedimientos establecidos por el Órgano Rector en materia de sistemas de información para el desarrollo de los mismos dentro del área.

14.2.2 Control: Procedimientos de control de cambios en los sistemas.

En el ciclo de vida de desarrollo se deberán hacer uso de procedimientos formales de control de cambios.

14.2.3 Control: Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Las aplicaciones críticas para el negocio se deberán revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad del área en su relación con las demás.

14.2.4 Control: Restricciones a los cambios en los paquetes de software

Se deberán tomar los recaudos necesarios a la hora de realizar modificaciones en los paquetes de software suministrados por terceros de acuerdo a lo permitido por la licencia obtenida. Todos los cambios se deberán controlar estrictamente.

14.2.5 Control: Uso de principios de ingeniería en protección de sistemas

Se deberán establecer, documentar, mantener y aplicar los principios de seguridad, como ser la integridad, disponibilidad y confidencialidad, para cualquier labor de implementación en el sistema de información.

14.2.6 Control: Seguridad en entornos de desarrollo

Las áreas deberán establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.

14.2.7 Control: Externalización en entornos de desarrollo

Las áreas deberán supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.

14.2.8 Control: Pruebas de funcionalidad durante el desarrollo de los sistemas

Se deberán realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.

14.2.9 Control: Pruebas de aceptación

Se deberán establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.

14.3 Categoría: Datos de prueba

Objetivo

Garantizar la protección de los datos que se utilizan para procesos de pruebas.

Se evitará la exposición de datos sensibles en entornos de prueba. Para proteger los datos de prueba se deberán establecer normas y procedimientos que contemplen prohibir el uso de bases de datos operativas.

14.3.1 Control: Protección de los datos utilizados en pruebas

Los datos de pruebas se deberán seleccionar cuidadosamente, proteger, controlar y sólo ser utilizados dentro del entorno de prueba.

15. Cláusula: Relaciones con suministradores

Generalidades

Los suministradores del área deben ser gestionados en lo que respecta a los aspectos de seguridad que tienen que ver con el establecimiento y el acuerdo de todos los requisitos de seguridad de la información del área.

Objetivo

Proteger la información del área que es accedida por los suministradores.
Establecer y mantener el nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos pre establecidos con el proveedor.
El área deberá chequear la implementación de los acuerdos, monitorear su cumplimiento con estándares definidos y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas.

Alcance

Esta política se aplica a todos los acuerdos con terceros suministradores que tengan o puedan tener acceso a datos de los sistemas de información del área.

Responsabilidad

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, deben definir en función a la criticidad de la información, los requerimientos de protección en lo referente al acceso de la información de los suministradores durante todo el período de relación contractual con el área. Asimismo todo responsable de las áreas legales, compras o que gestionen los contratos con suministradores, deben garantizar que en los mismos se definan y se pacten los niveles de seguridad establecidos por el área.

Política

15.1 Categoría: Seguridad de la información en las relaciones con suministradores

Objetivo

Garantizar y asegurar los activos de información del área que son utilizados por los suministradores, cumpliendo con el nivel de seguridad establecido.

15.1.1 Control: Política de seguridad de la información para suministradores.

Se deben acordar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los suministradores a los activos del área con el proveedor y se deben documentar debidamente.

El área debe identificar e imponer controles de seguridad de la información por medio de una política para abordar específicamente el acceso de los suministradores a la información del área.

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de equipamiento de Trabajo del Área contemplarán, mínimamente, los siguientes aspectos:

a) la identificación y la documentación de los tipos de suministradores, es decir, los servicios de TI, las utilidades de logística, los servicios financieros, los componentes de la infraestructura de TI y a quiénes autorizará el área para acceder a su información;
b) un proceso y ciclo de vida estandarizado para administrar las relaciones con los suministradores;
c) la definición de los tipos de acceso a la información, monitoreo y control de acceso que se les permitirá a los distintos tipos de suministradores;
d) requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso que será base de los acuerdos individuales con los suministradores de acuerdo a las necesidades del área, los requisitos y su perfil de riesgo;
e) procesos y procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión de terceros y la validación de productos;
f) controles de nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes;
g) obligaciones aplicables a los suministradores para proteger la información;
h) manejo de incidentes y contingencias asociadas con el acceso a los suministradores, incluidas las responsabilidades del área y los suministradores;

El área deberá tener en cuenta desde su organización:

a) resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información o el procesamiento de información proporcionado por cualquiera de las partes;
b) capacitación de concientización para el personal del área involucrado en las adquisiciones sobre políticas, procesos y procedimientos correspondientes;
c) capacitación de concientización para el personal del área que interactúa con el personal de los suministradores en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información del área;
d) que las condiciones sobre los controles y requisitos de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;
e) administración de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otro activo de información que se deba mover y, garantizando que se mantiene la seguridad de la información a través de todo el período de transición.

15.1.2 Control: Tratamiento del riesgo dentro de acuerdos con suministradores.

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información del área.

A continuación se añaden términos para incluir en los acuerdos a fin de poder satisfacer los requisitos de seguridad de la información identificados:

a) descripción de la información que se debe proporcionar o a la que se debe acceder y los métodos para proporcionar o acceder a la información;
b) clasificación de la información de acuerdo al esquema de clasificación del área; y si es necesario también realizar el mapeo entre el esquema propio del área y el esquema de clasificación del proveedor;
c) requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y una descripción de sobre cómo se garantizar su cumplimiento;
d) obligación de cada parte contractual de implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría;
e) reglas de uso aceptable de la información, incluido el uso inaceptable en caso de ser necesario;
f) una lista explícita del personal autorizado para acceder y/o recibir la información o los procedimientos o condiciones del área para su autorización y el retiro de la autorización, para el acceso y/o la recepción de la información del área al personal del proveedor;
g) políticas de seguridad de la información pertinentes al contrato específico;
h) requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes);
i) requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información, es decir, para la respuesta ante incidentes y procedimientos de autorización;
j) normativas pertinentes para la subcontratación, incluidos los controles que se deben implementar;
k) socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información;

l) requisitos de selección, si existe alguno, para el personal del proveedor para realizar los procedimientos de selección y notificación si no se ha completado la selección o si los resultados dan pie a dudas o inquietudes;
m) derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo;
n) procesos de resolución de defectos y resolución de conflictos;
o) obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe;
p) obligaciones del proveedor para cumplir con los requisitos de seguridad del área.

15.1.3 Control: Cadena de suministro en tecnologías de la información y comunicaciones.

Se deben incluir en los acuerdos con los suministradores, los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios.

Por lo que, en toda contratación o tercerización donde se deba establecer una cadena de suministros se debe contemplar:

a) definir los requisitos de seguridad de la información que se aplicarán a la adquisición de tecnologías, productos o servicios de información y comunicación además de los requisitos de seguridad de la información para las relaciones con el proveedor;
b) para los servicios de tecnología de información y comunicación, que requieren que los usuarios propaguen los requisitos de seguridad del área en toda la cadena de suministro si los suministradores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados al área;
c) para los productos de tecnología de información y comunicación que requieren que los suministradores propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro si estos productos incluyen componentes comprados a otros suministradores;
d) implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación se adhieren a los requisitos de seguridad establecidos;
e) implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando se desarrollan fuera del área, especialmente si el proveedor del nivel superior externaliza los aspectos de los componentes de productos o servicios a otros suministradores;
f) obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministros;
g) obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado sin ninguna función inesperada o no deseada;
h) definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier inconveniente entre el área y los suministradores;
i) implementación de procesos específicos para administrar el ciclo de vida de los componentes de tecnología de información y comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye los riesgos de los componentes que ya no están disponibles debido a que los suministradores ya no están en el negocio o a que ya no proporcionan estos componentes debido a los avances de la tecnología.

15.2 Categoría: Gestión de la prestación del servicio por suministradores

Objetivo

Mantener el nivel de seguridad de la información en la prestación de servicios conforme a los acuerdos con el proveedor en materia de seguridad de información.

15.2.1 Control: Supervisión y revisión de los servicios prestados por terceros

Se llevará a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad de la información y las condiciones definidas en los acuerdos, asegurando que los incidentes de seguridad de la información y los problemas son manejados en forma adecuada.

El área mantendrá control y visión general de todos los aspectos de seguridad para la información sensible o crítica, de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte.

15.2.2 Control: Gestión de cambios en los servicios prestados por terceros.

Durante el proceso de gestión de cambios, incluyendo el mantenimiento y mejoras de políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los sistemas y procesos del negocio involucrados, como así también la revaluación de los riesgos. Se deben contemplar los siguientes ítems:

- Los cambios realizados por la organización para implementar:
  - mejoras a los servicios corrientes ofrecidos;
  - desarrollo de cualquier aplicaciones y sistemas nuevos;
  - modificaciones o actualizaciones de las políticas y procedimientos del área;
  - nuevos controles para resolver los incidentes de la seguridad de la información y para mejorar la seguridad;
- cambios en los servicios de las terceras partes para implementar:
  - cambios y mejoras de las redes;
  - uso de nuevas tecnología
  - adopción de nuevos productos o nuevas versiones/publicaciones;
- nuevas herramientas de desarrollo y ambientes;
- cambios de las ubicaciones físicas de las instalaciones de servicio;
- cambio de los suministradores.

16. Cláusula: Gestión de incidentes en la seguridad de la información

Generalidades

Existen numerosas amenazas que atentan contra la seguridad de la información, representando riesgos latentes que de materializarse pueden ocasionar incidentes de seguridad.

Las áreas cuentan con innumerables activos de información, cada uno de los cuales puede encontrarse expuesto a sufrir incidentes de seguridad. Es por ello que resulta sumamente necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuras ocurrencias.

Objetivo

Garantizar que los eventos de seguridad de la información y las debilidades asociadas al manejo de los mismos, sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Alcance

La Política definida en este documento se aplica a todo incidente que pueda afectar la seguridad de la información del área.

Responsabilidad

El Comité Jurisdiccional de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad de la Información maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Seguridad de la Información y a los propietarios de la información Asimismo, el Responsable de Seguridad de la Información, el Responsable o Director del área y el Responsable del Área Recursos Humanos son responsables de comunicar fehacientemente los procedimientos de Gestión de Incidentes a todos los empleados sin importar la situación de revista de estos.

El Responsable Legal participará en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal del área es responsable de reportar debilidades e incidentes de seguridad que oportunamente se detecten.

Política

16.1 Categoría: Gestión de incidentes de seguridad de la información y mejoras.

Objetivo

Garantizar una administración de incidentes de seguridad de la información coherente y eficaz en base a un enfoque de comunicación de los eventos y las debilidades de seguridad.

16.1.1 Control: Responsabilidades y procedimientos.

Se establecerán responsabilidades y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems, en el caso de no tratarse de sistemas informáticos, completar solo el ítem que corresponda:

1. Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:
   a) Fallas operativas
   b) Código malicioso (exclusivo de sistemas informáticos)
   c) Intrusiones
   d) Fraude informático (exclusivo de sistemas informáticos)
   e) Error humano

f) Catástrofes naturales

2. Comunicar formalmente los incidentes a través de autoridades o canales apropiados tan pronto como sea posible.
3. Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):
   a) Definición de las primeras medidas a implementar.
   b) Análisis e identificación de la causa del incidente.
   c) Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
   d) Comunicación formal con las personas afectadas o involucradas con la recuperación del incidente.
   e) Notificación de la acción a la autoridad y/o áreas pertinentes.
4. Registrar pistas de auditoría y evidencia similar para:
   a) Análisis de problemas internos.
   b) Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.
5. Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
   a) Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
   b) Documentación de todas las acciones de emergencia emprendidas en forma detallada.
   c) Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
   d) Constatación de la integridad de los controles y sistemas del área en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del Responsable Legal del Organismo en el tratamiento de incidentes de seguridad ocurridos, y de ser necesario se iniciarán los procedimientos administrativos de investigación/sanción que correspondientes

16.1.2 Control: Notificación de los eventos de seguridad de la información.

Los incidentes relativos a la seguridad serán comunicados a través de las autoridades o canales apropiados tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre la ocurrencia de éstos.

El procedimiento debe contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad de la Información sea notificado tan pronto como sea posible. Este, en conjunto con el Director del área o la máxima autoridad, comunicarán a las áreas responsables de investigar dependiendo del incidente (Poder Judicial, FIA, Contaduría General, o quien corresponda).

Asimismo, mantendrá al Comité Jurisdiccional de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Todos los empleados y contratistas deben conocer fehacientemente el procedimiento de comunicación de incidentes de seguridad, y deben informar formalmente los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

16.1.3 Control: Notificación de los puntos débiles de la seguridad.

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente de una debilidad de seguridad, son responsables de registrar y comunicar formalmente las mismas al Responsable de Seguridad de la Información.

Se prohíbe expresamente a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

16.1.4 Control: Valoración de eventos de seguridad de la información y toma de decisiones.

Los eventos de seguridad deberán ser evaluados con el fin de permitir su clasificación con respecto a su nivel de criticidad.

16.1.5 Control: Respuesta a los incidentes de seguridad.

Se deberá responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.

16.1.6 Control: Aprendizaje de los incidentes de seguridad de la información.

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

16.1.7 Control: Recopilación de evidencias.

El área deberá definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia ante la ocurrencia de incidentes respetando las competencias de otros organismos como Poder Judicial, Policía, Organismos de Contralor y Rectores del Poder Ejecutivo Provincial.

17. Cláusula: Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del área.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del área puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados, transformarse en una parte integral del resto de los procesos de administración y gestión, incluyendo controles destinados a identificar y reducir riesgos, atenuando las consecuencias de eventuales interrupciones de las actividades del área y asegurando la reanudación oportuna de las operaciones indispensables.

Objetivo

Mantener la seguridad de la información integrada a la gestión de la continuidad del negocio del área, es decir, preservarla durante las fases de activación, desarrollo de procesos, procedimientos y planes para la continuidad de negocio y reanudación de actividades. Como así también, minimizar los efectos de las posibles interrupciones de las actividades normales del área (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Maximizar la efectividad de las operaciones de contingencia del área con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) Notificación/Activación: Consistente en la detección y determinación del daño y la activación del plan.
b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido.
c) Recuperación: Consistente en la restauración de las capacidades de proceso a las condiciones de operación normales.

Asegurar la coordinación con el personal del área y los contactos externos que participarán en las estrategias de planificación de contingencias. Especificar funciones para cada actividad definida.

Alcance

Esta Política se aplica a todos los procesos críticos identificados en el área.

Responsabilidad

El Responsable de Seguridad de la Información participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información y el Responsable de Seguridad de la Información cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del área.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del área.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del área.

Se deberán tomar las medidas necesarias para asegurar la verificación en el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité Jurisdiccional de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del área frente a interrupciones imprevistas.

Política

17.1 Categoría: Continuidad de la seguridad de la información.

Objetivo

Contrarrestar las interrupciones a las actividades del área y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

17.1.1 Control: Planificación de la continuidad de la seguridad de la información.

Este Responsable de Seguridad tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del área frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

a) Identificar y priorizar los procesos críticos de las actividades del área.
b) Asegurar que todos los integrantes del área comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en las actividades.
c) Elaborar y documentar una estrategia de continuidad de las actividades del área consecuente con los objetivos y prioridades acordados.
d) Proponer planes de continuidad de las actividades del área de conformidad con la estrategia acordada.
e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones y roles para su cumplimiento.
f) Coordinar actualizaciones periódicas de los planes y procesos implementados.
g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del área.
h) Proponer las modificaciones a los planes de contingencia.

17.1.2 Control: Implantación de la continuidad de la seguridad de la información.

Quienes participan de los procesos y administran recursos de información, con la asistencia del Responsable de Seguridad de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del área. Estos procesos deben ser propuestos por el Comité Jurisdiccional de Seguridad de la Información.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
d) Documentar los procedimientos y procesos acordados.
e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
f) instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:
    - Objetivo del plan.
    - Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
    - Procedimientos de divulgación.

- Requisitos de la seguridad.
- Procesos específicos para el personal involucrado.
- Responsabilidades individuales.

g) Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades requeridas del área, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

17.1.3 Control: Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Se deberán verificar de manera regular los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante las adversidades.

17.2 Categoría: Redundancias.

Objetivo

Garantizar la disponibilidad de las instalaciones de procesamiento de información.

17.2.1 Control: Disponibilidad de instalaciones para el procesamiento de la información.

Se deben implementar la suficiente redundancia en las instalaciones de procesamiento de la información, en correspondencia con los requisitos de disponibilidad.

Para cumplir con lo anterior el área debe identificar los requisitos funcionales para considerar los componentes o arquitecturas redundantes. Hay que tener en cuenta durante el diseño, la actividad de la gestión de los riesgos de integridad y confidencialidad de la información.

18. Cláusula: Cumplimiento

Generalidades

El diseño, operación, uso y administración de la información, así como su mal uso están regulados por disposiciones, decretos y leyes.

Los requisitos normativos y contractuales pertinentes al manejo o desarrollo del conjunto de la información, deben estar debidamente definidos y documentados.

Objetivo

Evitar incumplimientos a las disposiciones normativas y contractuales a fin de evitar sanciones administrativas, civiles o penales.

Garantizar que la administración y uso de la información cumplan con la política, normas y procedimientos de seguridad del área.

Revisar la seguridad de la información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad.

Alcance

Esta Política se aplica a todo el personal del área, cualquiera sea su vínculo con el estado.

Responsabilidad

El Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Realizar revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.
- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

El Responsable Legal del área o quien a su vez cumpla la función, con la asistencia del Responsable de Seguridad de la Información cumplirán las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para el uso y administración de la información.

Todos los empleados sin importar su vínculo con el Estado en especial los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

Política

18.1 Categoría: Cumplimiento de los requisitos legales y contractuales

Objetivo

Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

El diseño, operación, uso y gestión de la información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.

18.1.1 Control: Identificación de la legislación aplicable.

Se deberán identificar, documentar y mantener al día, de manera explícita todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque del área para cumplir con estos requisitos.

18.1.2 Control: Derechos de propiedad intelectual (DPI).

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deben tener presentes las siguientes normas:

- Ley de Propiedad Intelectual N° 11.723 y sus modificatorias: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.
- Ley de Marcas N° 22.362 y sus modificatorias: Protege la propiedad de una marca y la exclusividad de su uso.
- Ley de Patentes de Invención y Modelos de Utilidad N° 24.481: Protege el derecho del titular de la patente de invención a impedir que terceros utilicen su producto o procedimiento.

Derecho de Propiedad intelectual del Software

- El software es considerado una obra intelectual que goza de la protección de la Ley 11.723 de Propiedad Intelectual.

18.1.3 Control: Protección de los registros de la organización.

Los registros críticos del área se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del área.

Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos.

Tipo de registro	Periodo de retención	Medio de almacenamiento	Responsable

Se considerarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
c) Implementar controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

En particular, se deben tener presente las siguientes normas:

- Estatuto del Empleado Público. Ley Provincial N° 292-A (Antes Ley N° 2.017): Establece que las personas que se desempeñen en la función pública deben proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- Código Penal Art. 255: Sanciona con prisión de un (1) mes a cuatro (4) años, a quien sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
- Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($750) a pesos doce mil quinientos ($12.500)
- Ley N° 24.624. Artículo 30: Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional y otorga valor jurídico y probatorio a la documentación existente que se incorpore al Archivo General de la Administración, mediante la utilización de tecnología que garantice la estabilidad, perdurabilidad, inmutabilidad e inalterabilidad del soporte de guarda físico de la mencionada documentación.
- Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo las compilaciones de datos o de otros materiales.
- Ley N° 25.506: Establece que la exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.
- Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183).

18.1.4 Control: Protección de datos y privacidad de la información personal.

Se deberá garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.

Todos los empleados deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

En particular, se deben tener presente las siguientes normas:

- Protección de Datos Personales. Ley 25.326: Establece responsabilidades para aquellas personas que recopilan, procesan y divulgan información personal y define criterios para procesar datos personales o cederlos a terceros.
- Confidencialidad. Ley N° 24.766: Impide la divulgación a terceros, o su utilización sin previo consentimiento y de manera contraria a los usos comerciales honestos, de información secreta y con valor comercial que haya sido objeto de medidas razonables para mantenerla secreta.
- Código Penal: Sanciona a aquel que abriere, accediere o se apoderare indebidamente, entre otros, una comunicación electrónica; o suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.(Art. 153); a aquel que accediere en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios financieros. (Art. 153 bis 2°p); al que el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. (Art. 155); al que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa

(Art. 156); al funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos (Art. 157); al que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales, ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley o ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales (Art. 157 bis); al que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183); al que revelare secretos políticos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, o al que por imprudencia o negligencia diere a conocer los secretos mencionados anteriormente, de los que se hallare en posesión en virtud de su empleo u oficio (Art. 222 y 223).

18.1.5 Control: Regulación de los controles criptográficos.

Se deberán utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

18.2 Categoría: Revisiones de la seguridad de la información.

Objetivo

Asegurar el cumplimiento de las políticas y estándares de seguridad organizacional.
La seguridad de la información se debiera revisar regularmente.
Estas revisiones deben realizarse en base a las políticas de seguridad apropiadas y las plataformas técnicas.

18.2.1 Control: Revisión independiente de la seguridad de la información.

Se deberá revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.

18.2.2 Control: Cumplimiento de las políticas y normas de seguridad.

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad de la Información, realizará revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.
b) Proveedores de sistemas.
c) Propietarios de información.
d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

18.2.3 Control: Comprobación del cumplimiento.

Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.